УДК 343.98

***М. Г. Жук***
*доцент кафедры уголовного права, уголовного процесса и криминалистики Гродненского государственного университета им. Янки Купалы, кандидат юридических наук, доцент*

# ПРОБЛЕМНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Цифровые технологии являются неотъемлемой частью нашей жизни и могут способствовать подготовке, совершению и сокрытию преступления.

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности: повышенная латентность совершения преступлений; трансграничный характер сетевых преступлений; интеллектуальный характер преступной деятельности; возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно; многоэпизодный характер; неосведомленность потерпевших; порой невозможность предотвращения и пресечения преступлений данного вида традиционными средствами [1, с. 46].

Получение и анализ доказательств по делам о преступлениях в сфере компьютерной информации — одна из основных и труднорешаемых на практике задач. Ее решение требует не только особой тактики проведения следственных и организационных мероприятий, но и наличия специальных познаний в области компьютерной техники и программного обеспечения. При расследовании компьютерных преступлений следователь сталкивается с необходимостью выявления и изъятия следов, собирания доказательств на таких объектах исследования, как компьютерная система, телекоммуникационная сеть или носитель информации (магнитный, оптический и т. д.). При этом в некоторых случаях приходится искать нечто неосязаемое, а не привычные физические улики в виде следов применения оружия, отпечатков пальцев, поддельных документов. Основные проблемы связаны с описанием подлежащего изъятию компьютерного оборудования и компьютерной информации, а также с тактикой проведения обыска. Особые сложности при производстве следственных действий возникают в случае распределенных компьютерных систем обработки информации, так как место совершения преступления часто не совпадает с местом происшествия и наступления преступного результата [2, с. 265–270].

По нашему мнению, алгоритм расследования преступлений в сфере высоких технологий может включать следующие этапы:

1) установление самого факта неправомерного доступа к информации в компьютерной системе или сети; 2) установление места несанкционированного проникновения в компьютерную систему или сеть; 3) установление времени несанкционированного доступа; 4) установление надежности средств защиты компьютерной информации; 5) установление способа несанкционированного доступа; 6) установление лиц, совершивших неправомерный доступ к компьютерной информации; 7) установление виновности и мотивов лиц, совершивших неправомерный доступ к компьютерной информации; 8) установление вредных последствий неправомерного доступа к компьютерной системе или сети; 9) выявление обстоятельств, способствовавших неправомерному доступу к компьютерной информации [3, с. 158].

На первоначальных этапах предварительного расследования по уголовным делам данной категории важным видится проведение следующих следственных действий: допрос потерпевших и свидетелей, выемка технических устройств (персональных компьютеров и мобильных телефонов), осмотр данных устройств и компьютерной информации, содержащейся на них.

Данные следственные действия являются важными при проведении предварительного расследования по уголовному делу на первоначальных этапах, так как необходима незамедлительная фиксация информационных следов преступления (никнеймы, фишинговые сайты, IP-адреса) ввиду того, что данные следы с учетом времени могут быть удалены или видоизменены, что повлечет их утрату и тем самым невозможность объективно и оперативно проводить предварительное расследование по уголовному делу.

Работа следователя по уголовным делам, например возбужденным по ст. 349 Уголовного кодекса Республики Беларусь, в большей степени заключается в проведении осмотра и анализа компьютерной информации и иных документальных сведений, полученных в ходе предварительного расследования по уголовному делу. Следует допросить потерпевших и свидетелей, которые более детально помнят события совершенного преступления и от которых можно получить наиболее достоверную информацию. В процессе расследования уголовного дела следователю в целях сбора дополнительных доказательств — в случае, если установлено лицо, причастное к совершению преступления, а также — установления лица, совершившего преступление — в случае его отсутствия, необходимо тесное сотрудничество с органом дознания, который имеет право проведения оперативно-розыскных и поисковых мероприятий.

В рамках реализации данного сотрудничества на основании ч. 7 ст. 36 Уголовно-процессуального кодекса Республики Беларусь следователь

направляет в орган дознания поручение, в котором указывает действия, которые необходимо выполнить по уголовному делу, после чего сотрудник органа дознания, которому поручается исполнение поручения, в течение 10 суток должен исполнить поручение, а при невозможности его исполнения в срок — уведомить следователя.

По своему характеру преступления в сфере высоких технологий совершаются в течение короткого промежутка времени и, как правило, удаленно. При совершении данного вида преступлений злоумышленник имеет в своем распоряжении богатый арсенал технических и программных средств, которые упрощают его деятельность и, помимо прочего, дают ему возможность маскировать следы преступления. У следователя или оперативного сотрудника, чтобы зафиксировать указанные следы, в распоряжении имеется мало времени, а зачастую затруднены как технические, так и законные возможности выполнить те или иные следственные действия в данный момент, например при получении сведений в организации, банке, в другом государственном органе, для чего требуется подготовка официального запроса, а в случае, если запрашиваемая информация составляет охраняемую законом тайну, — еще и санкция прокурора, срок предварительного расследования в таких случаях затягивается, что обуславливается ожиданием получения ответа на запрос. На законодательном уровне установлен срок исполнения запроса в 15 суток, однако он зачастую нарушается исполнителями ввиду служебной загруженности, что увеличивает срок предварительного расследования.

Таким образом, успех расследования преступлений данной категории зависит от оперативного взаимодействия государственных органов и организаций внутри страны; от правильно выбранного алгоритма расследования; от применения современных технико-криминалистических средств и от сотрудничества правоохранительных органов разных государств.

**Список основных источников**

1. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45–55. Вернуться к статье

2. Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5. С. 265–270. Вернуться к статье

3. Жук М. Г. Формирование криминалистической методики расследования преступлений в сфере высоких технологий [Электронный ресурс] // I Минские криминалистические чтения : материалы Междунар. науч.-практ. конф., Минск, 20 дек. 2018 г. : в 2 ч. / Акад. М-ва внутр. дел Респ. Беларусь. Минск, 2018. Ч. 1. С. 154–159. Вернуться к статье